Before the
FEDERAL COMMUNICATIONS COMMISSION
Washington, DC 20554

In the Matter of	)	
	)	CC Docket No. 93-292
Policies and Rules	)	
Concerning Toll Fraud	)	

COMMENTS OF U S WEST COMMUNICATIONS, INC.

Kathryn Marie Krause
Suite 700
1020 19th Street, N.W.
Washington, DC 20036
(303) 672-2859

Attorney for

U S WEST COMMUNICATIONS, INC.

Of Counsel,
Laurie J. Bennett

January 14, 1994

TABLE OF CONTENTS

SUMMARY

Telecommunications fraud is a serious problem. But, it is not a problem being ignored or taken casually. Telecommunications providers, CPE manufacturers, entrepreneurs, industry associations and law enforcement personnel are all working together to devise better fraud prevention mechanisms.

The work of these entities should be applauded, not duplicated. Thus, the Commission's focus should be on whether there is anything it can do by rulemaking that can enhance the fraud prevention activities already in existence. U S WEST does not believe that there is.

With regard to LECs in particular, U S WEST is confident that filed comments will resemble our own in detailing the already extensive work being done to prevent and control fraud, ranging from customer education to the development of network access and screening mechanisms. We are confident that the evidence submitted will debunk any theory that LECs are not sufficiently pro-active in the area of fraud prevention because they enjoy a limited liability with respect to fraud liability.

The Commission should not manipulate carriers' existing tariff limitations of liability with respect to fraud liability, for at least two reasons. First, limitations of liability are of broad application and should not be required to be changed for a particular class of customer with a particular kind of problem. Second, carriers' existing limitations of liability currently operate with regard to fraud in a manner properly aligned with

sound risk management principles, both with regard to prevention and loss liability. The entity that either controls or has responsibility for the CPE originating or terminating a telecommunications transaction should be the responsibility (and attendant costs) associated with that access. While LECs can aid customers in controlling such access, they cannot make choices for them, or guarantee against human conduct or behavior, especially conduct criminal in nature.

For the above reasons, U S WEST submits that the Commission need not proceed further with this proceeding, other than to encourage current fraud prevention efforts to remain robust. It might also wish to set up some kind of internal bureaucratic mechanism so that it receives minutes of industry association meetings, or the like, in order to remain well informed of the ongoing fraud prevention activities.

Like many other telecommunications issues, U S WEST believes that the marketplace and the industrious conduct of the players in that marketplace will provide resolution of certain fraud problems. It will not eliminate them, to be sure. The world of electronics, computers and digital communications brings with it its own inherent intrigue to those interested in free carriage. Those interested in carriage for a fee will remain motivated to design and deploy networks capable of rendering to them amounts properly due and owing. There is probably no regulatory motivator more forceful than that.

For the above reasons, U S WEST would encourage the Commission to reflect seriously on whether or not the current docket needs to be extended beyond the instant pleading phase (i.e., comments and replies). If it is demonstrated that nothing materially helpful can be done by allowing the proceeding to remain open and that no rules need to be promulgated, U S WEST would encourage the Commission to terminate the proceeding.

Before the
FEDERAL COMMUNICATIONS COMMISSION
Washington, DC 20554

In the Matter of	)	
	)	CC Docket No. 93-292
Policies and Rules	)	
Concerning Toll Fraud	)	

COMMENTS OF U S WEST COMMUNICATIONS, INC.[1]

I. INTRODUCTION

The Federal Communications Commission's ("Commission") concern about telecommunications fraud[2] is understandable. The scope, technology and financial responsibility issues associated with telecommunications fraud are matters that should be of concern to the primary interstate agency dealing with telecommunications issues and policies.

---

[1]U S WEST Communications, Inc. ("U S WEST"), is filing these comments on behalf of ourselves, i.e., the telephone operating company, and with a voice not inconsistent with the interests of our other affiliated companies. Our cellular company, U S WEST NewVector Group, Inc., is filing comments on its own behalf through its trade association, the Cellular Telephone Industry Association ("CTIA"). Thus, these comments do not address any aspect of cellular fraud, with respect to either its prevention or liability.

[2]In the caption of the Commission's Notice of Proposed Rulemaking in this proceeding, the Commission references "toll" fraud. In the Matter of Policies and Rules Concerning Toll Fraud, CC Docket No. 93-292, Notice of Proposed Rulemaking, FCC 93-496, rel. Dec. 2, 1993 ("NPRM"). However, as the text of the NPRM makes clear, the matter goes beyond toll fraud, especially within the context of cellular and other wireless carriers. And see the Commission's use of the phrase "telecommunications fraud" early in the NPRM ¶ 2. Thus, throughout these comments U S WEST addresses the broader issue, focusing on toll fraud only in those circumstances where the restricted term is appropriate.

U S WEST shares the Commission's concern about such fraud. We have taken active steps, with regard to both our customers and industry groups to educate them about the risks of telecommunications fraud and to fashion products and services to aid customers in their attempts to control fraud. We believe that we are highly regarded in the industry for our efforts, and we describe those efforts in more detail below.

Notwithstanding our endorsement of the Commission's concern about telecommunications fraud, however, we are uncertain that a rulemaking proceeding, for the ultimate promulgation of rules, is the appropriate forum for resolution of the fraud problem. Clearly, the Commission has the authority to require printed warnings on customer premises equipment ("CPE"),[3] and to require verbal warnings at the time of sale of either CPE or various telecommunications services.[4] Clearly, under certain circumstances the Commission has the authority to manipulate limitations of liability as between carriers and customers.[5] But whether such actions should be taken should depend as much on the actual efficacy of such actions in the real marketplace as on the theoretical or ideological public policy benefits presumed to inure from them.

When a regulatory or bureaucratic agency attempts to solve a problem, especially one as complex as telecommunications fraud

---

[3] Id. ¶¶ 1, 40.

[4] Id. ¶¶ 24-25.

[5] Id. ¶ 41.

(dependent as it is on the conjunction of technology and malevolent behaviors), by "rulemaking to the problem," certain consequences are predictable. First, the "problem" is often inaccurately identified or defined. Second, someone somewhere will figure out how to get around the rule or how to craft a technology not bound by it.

Thus, U S WEST would support the Commission's establishment of policies or principles regarding telecommunications fraud, rather than the promulgation of rules. The establishment of policies is the most appropriate regulatory response to telecommunications fraud, perhaps with certain presumptions associated with conformity (or lack of conformity) with such principles.[6]

The establishment of principles, rather than the promulgation of agency rules, would also meld well with marketplace activity. It is not just the Commission that is concerned about telecommunications fraud. The Commission's NPRM itself identifies various agencies and industry groups which are aggressively working toward solutions to the moving target[7] of telecommunications fraud. And, undoubtedly, comments in this proceeding will provide further information to enlighten the Commission on

---

[6]The Commission has identified its purpose in this proceeding to be "to identify additional policies we should establish or steps we should take to avoid, or reduce the risks of, toll fraud." Id. ¶ 10.

[7]Id. ¶¶ 5, 7 n.7.

various company initiatives and activities directed toward fraud reduction.[8]

None of this work, however, will ever totally eliminate telecommunications fraud, any more than department stores can eliminate shoplifting. The costs of such criminal activity have become costs of doing business, costs that the general consuming population pays for -- whether due to increased uncollectibles or increased security and prevention activities. And, in much the same way that self-service department stores create greater customer choice and flexibility (at least theoretically), while at the same time creating more attractive "self-service" for shoplifters as well,[9] the same telecommunications technology that allows for equal access and that, in the future, will support callers on the move (such as personal communications services ("PCS"), etc.) will also create the environment in which persons of malicious intent will be able to commit fraud.[10]

Thus, one of the most fundamental considerations that faces the Commission from a policy perspective is <u>where</u> and <u>how</u> the

---

[8]The Commission's observation that "[i]t does not appear, however, that private action can resolve all toll fraud problems" is, undoubtedly, correct. <u>Id.</u> ¶ 8. <u>No</u> one segment can resolve all toll fraud problems. That should not, however, demean or diminish the tremendous strides being made in the private sector in this regard.

[9]Thus necessitating increased security measures such as cameras, permanently-attached clothing tags and bar codes, etc.

[10]<u>Compare</u> the Commission's observation that "[e]xperience has shown that those new telecommunications technologies offering the most convenience and flexibility for users, are often also most likely to present new toll fraud opportunities." <u>NPRM</u> ¶ 5.

"fraud costs" of the telecommunications business should be recovered. It is not apparent that any reallocation of those costs is necessary or desirable, as it currently appears that both the costs of fraud prevention and fraud liability are lodged appropriately.

The "costs" of fraud in the telecommunications business are comprised of two distinct components: the costs associated with attempts to prevent and/or control fraudulent conduct in the first instance (i.e., prophylactic costs); and those costs associated with completed fraudulent activity (i.e., liability costs). The Commission expresses an interest in understanding the way in which those costs might be correlated.[11] It suggests that responsibility for liability costs might create a direct incentive to incur fraud prevention costs.[12]

While the theory associated with such a risk management analysis might have some validity, the context in which the theory is analyzed is critical. And here the context is disturbing.

The suggestion is that if carriers were held liable for fraud losses, they would have incentives to build more fraud prevention features/functions into their networks. And, conversely, if carriers are not held financially responsible for such losses, they will behave in a cavalier, uninterested manner

---

[11] Id. ¶¶ 24, 41. See also the separate statement of Commissioner Andrew C. Barrett released with the NPRM.

[12] Id. ¶ 41.

with regard to fraud prevention. As is made evident from the information presented below, while the former proposition might hold some theoretical appeal, the total lack of accuracy of the converse proposition demonstrates the logical flaw in the suggestion itself.

Carriers already have incentives to make their networks as secure from fraud as possible, from both their own internal self-interest (i.e., uncollectibles), as well as from a customer-service perspective. Furthermore, the various industry activities and product solutions discussed throughout the text of this filing themselves demonstrate that the commitment of substantial resources (both time and money) is already being incurred by carriers with regard to fraud prevention, despite and regardless of their existing limited liability.

But more fundamentally, the theoretical suggestion that carriers would be more interested in preventing fraud if they were required to bear more of the losses is most disturbing in that it never really focuses on certain predicate questions: Should carriers be more liable? What entity is in the best position to control/prevent fraud? Are current prevention/liability principles actually correctly aligned with responsibility and control?

In all circumstances access to the network begins with a telephone or some other piece of CPE. In many ways, it is self-evident that the entity holding the keys to network access should bear the primary responsibility for the access accomplished. As

a fundamental principle of risk management, then, the entity with the care, custody and control of the CPE clearly should be the entity primarily responsible for either incurring the costs of prevention or absorbing the liability loss.

And, it should be remembered that, given the fact that customers are free purchasing agents, how they choose to allocate their resources will vary from purchaser to purchaser. Those that are less risk adverse may spend more money on prevention (i.e., purchasing the most state-of-the-art equipment); those that are comfortable assuming greater risk may bet on the liability come. But, in both cases, competition has been heralded as the harbinger of this kind of customer choice. Carriers should not be expected to cover for customers making Choice A over Choice B.[13]

With the increase in competition and the need to focus scarce resources on the business of the business, carriers should not be expected to become insurers against fraud perpetrated on their customers. Local exchange carriers ("LEC"), in particular, should not be viewed as some kind of "first line of protection"

---

[13]To return to the department store example, the suggestion that carriers should -- as a matter of regulatory rule or policy -- be the insurers against fraud perpetrated on customers is akin to suggesting that a department store owner who chooses not to purchase security cameras, or to hire security guards, and who declines to somehow secure easily-tagged merchandise, should be able to recover from the landlord or the electric company for its fraud losses because the premises did not come equipped with security cameras or security guards and the registers had no scanning equipment. The suggestion is absurd.

with regard to interstate message toll fraud.[14] While LECs are clearly acting as advocates against toll fraud, and are deeply immersed in customer education and fraud reduction programs, their willingness to create internal network fraud control devices will, of necessity, be driven by market conditions -- including demand and a willingness to pay for such features/ functions. Today, often, neither are present.

That is not to say that carriers are disinterested or neglectful of customer needs with regard to fraud prevention. The contrary is clearly the case. But it is to say that customer choice with regard to fraud controls and prevention will be accorded the same kind of marketplace resolution as other purchasing phenomena: customers will be permitted to choose and will get what they pay for.

The marketplace is fast addressing fraud. Some LECs, such as U S WEST, work closely with their customers to become more alert to potentially fraudulent activity, to design products and services that aid customers in making determinations about fraudulent practices or patterns, to warn customers who purchase CPE about the frailty of such systems (especially against agents hell-bent on breaking into them to engage in fraudulent

---

[14]U S WEST incurs minimal intraLATA toll fraud. And fraud that occurs as a result of the use of our calling card in conjunction with interstate calls could, in almost all circumstances, be reduced or controlled through the actions of the cardholder and the actions of interexchange carriers ("IXC") and operator service providers ("OSP") in verifying the card in our Line Information Database ("LIDB") offering.

activity). Other companies simply price their products very high to cover the cost of fraud, and still have purchasers.[15]

In the future, and with the increase in competition at both the toll level and increasingly with other telecommunications services (such as local exchange and enhanced services), fraud prevention will become, without a doubt, a marketing weapon and tool. Companies will sell themselves as leaders in preventing fraud or, alternatively, will sell their wares at a price that covers the fraud but which will still be attractive to certain buyers. Both network providers and their subtending customers will make decisions with regard to their acceptable risk aversion level as it pertains to fraud. Essentially, the marketplace will be a material contender in how telecommunications fraud is resolved. It will do so without the benefit of any manipulation of sound principles of risk management by the Commission.

Thus, U S WEST supports a marketplace resolution to telecommunications fraud. Industry groups will continue to meet to address how such fraud can be controlled, through either technology, warnings or criminal prosecutions. Governmental agencies will continue to work with carriers of various kinds to determine how to find and prosecute such fraud. Customers (especially sophisticated business customers) will become increasingly aware of the risks they run when they purchase CPE or certain

---

[15]This can be seen in some of the 900 "call collect" offerings where the price of the product is very high (reflective of the uncollectibles), but the volume of calls, apparently, covers the cost of the fraud.

telecommunications services, and will make intelligent (though not similar) choices about their level of risk aversion.

The Commission's role should be to set policy in this area, if any Commission action is necessary at all. It should endorse all industry and carrier initiatives associated with fraud prevention. It should encourage, although not mandate, the development of technologies that make fraudulent behavior more difficult. And, if necessary (which U S WEST is not confident about), it should articulate certain expected standards of behavior for various parties to telecommunications transactions. But, beyond that, the Commission should remain inactive, except in its role as judicial resolver of complaints.

II. U S WEST'S EFFORTS IN THE AREA OF FRAUD CONTROL AND PREVENTION

For almost a decade U S WEST has been an active participant in industry fora associated with fraud prevention. We also have an internal fraud committee that works closely with various parts of the U S WEST organization, and with other interested LECs and IXCs, to share information and work toward fraud control solutions. Indeed, U S WEST's fraud prevention programs have been praised: "U S WEST has the vision to address the issue and has a flourishing program for business customer education."[16]

---

[16]Dave Jordan, MCI fraud expert, at a Toll Fraud Prevention Committee meeting, Phoenix, AZ, November 3-4, 1993. See U S WEST Today, Nov. 15, 1993, attached hereto as Appendix A.

Additionally, U S WEST has developed certain access control, screening, and alternate billing products and services that can be used by customers to aid them in controlling access to the network, and consequentially, to the happenstance of fraud. When fraud does occur, U S WEST works actively with law enforcement to locate the perpetrators of fraud and to bring them to justice.

None of these fraud prevention activities is without costs. Today U S WEST expends substantial resources (both in terms of time and money) on the matter of fraud prevention, even though our liability for any ultimate fraud losses are limited. The suggestion that we might fall short on the fraud prevention side because we do not bear the loss of fraud on the liability side cannot be supported.

A. Participant in Industry Organizations

1. Toll Fraud Prevention Committee ("TFPC")

U S WEST has representation on the TFPC, which the Commission references in its NPRM.[17] That committee is a voluntary one, comprised of representatives from LECs, IXCs, cellular companies, switch vendors, state public utility commissions ("PUC"), and this Commission.

---

[17] NPRM ¶ 7 n.7. The TFPC is an association formed in 1987 under the auspices of the Network Operations Forum, one of the three interindustry forums under the organization formerly known as the Exchange Carriers Standards Association, now known as the Alliance for Telecommunications Industry Solutions.

This national forum gives industry representatives the opportunity to discuss different toll fraud detection and deterrence measures that are conceivable and/or are being implemented across the country by various CPE and service providers. The exchange of this kind of information is invaluable in the industry's efforts to deploy fraud deterrence and detection mechanisms. The organization is also instrumental in the design and delivery of industry and customer education efforts.

During the past six years, the TFPC has resolved 17 issues brought to it by its various constituents, including such matters as incoming international to collect coin fraud, third-number billing fraud and incoming collect to cellular fraud. It has also issued a white paper on subscription fraud.[18] Current issues under discussion by the TFPC include coin originating toll fraud, call forwarding fraud, local network hacking, potential fraud associated with Billed Party Preference and inmate lines, and Telecommunications Relay Service ("TRS") fraud.

2. Communications Fraud Control Association ("CFCA")

The CFCA is a national association with extensive membership among carriers, equipment vendors, business, government, and law enforcement organizations.[19] U S WEST has been active in the

---

[18]Subscription fraud is the establishment of service by a customer with a pre-existing intention not to pay for service. The service may be, variously, local exchange, toll, cellular, radio or some other kind of service.

[19]NPRM ¶ 7 n.7.

CFCA since its inception, and we are proud to say that one of our employees is the only CFCA board member from a former Bell Operating Company ("BOC").

The CFCA maintains a fraud alert network which provides updated bulletins that educate and warn members (including law enforcement agencies) of potential fraudulent trends and activities being detected across the country. Participation with CFCA provides U S WEST the opportunity to work with other telecommunications providers and law enforcement agencies to jointly pursue both legal and industry solutions to ever-changing fraud occurrences.

As is obvious, the kind of industry fora above discussed always have a full plate, and are constantly striving -- through cooperative efforts -- to come up with best practices associated with toll fraud prevention and control. It is hard to conceive of a formal regulatory operation that could do better work in this area. While the Commission should certainly applaud the efforts of such organizations, and should participate in as active a role as resource constraints permit, it should not try to duplicate already successful industry efforts in the area of fraud prevention and control.[20]

---

[20]Thus, U S WEST does support the establishment of a "new Federal Advisory Committee" on fraud. Compare id. ¶ 13.

B. U S WEST's Internal Telecommunications Fraud Committee

In addition to our work with various industry fora, we have an internal fraud committee that peruses the output of both industry fora and customers' expressed needs (including residential users, small businesses, large businesses, government users and carriers). This committee has representation from various departments[21] and meets periodically to review customer needs, to identify fraud control measures being undertaken both internally and by other companies, and to resolve upon future fraud control efforts and activities that should be pursued by U S WEST.

When necessary, appropriate subcommittees are formed to address specific "kinds" of fraudulent behaviors or patterns (e.g., subscription fraud, PBX fraud, payphone and Customer Owned Coin Operated Telephones ("COCOT") fraud, operator-handled fraud, etc.). Representatives from this committee have organized presentations for IXCs, large businesses and governmental users regarding fraud issues,[22] and continually work with other LECs and IXCs to explore and develop effective fraud control and prevention mechanisms.

As a part of the work of this internal committee, an e-mail notification system was established in U S WEST to immediately

---

[21]The committee has, in addition to those persons who are representatives on national committees, individuals from U S WEST's carrier, network, marketing, finance, security, and planning organizations.

[22]See further discussion below at 28-30.

inform U S WEST market units and other affected organizations within U S WEST of developing toll scams. U S WEST has made this e-mail network available to interested carriers, and we have also set up mechanisms to allow us to receive information from carriers into this network. This kind of close cooperation is essential for the successful management of toll fraud.

C. Products and Services

1. Services Designed for End Users

U S WEST has a number of products and services that we make available to customers to aid them in controlling access to and within the telecommunications network. With regard to our residential and small business customers, U S WEST does not actively promote fraud or telecommunications restriction services, unless a customer expresses some need or concern that would prompt a discussion about such services. The vast majority of our residential and small business customers have no need for such products, and discussions about them would only consume valuable business office and service order time and resources. However, if a customer suggests or conveys a need for such products,[23] U S WEST works closely with that customer to tailor

[23]This is usually the result of behavior unanticipated by the station owner, such as inappropriate calling by children or third parties who have accessed the home pursuant to some kind of invitation. Or it might be an employee suspected of workplace malfeasance.

restriction and control services to that customer's individual needs.

On the other hand, in the spirit of consultative telecommunications service provisioning, U S WEST does affirmatively discuss fraud issues with our large business and governmental customers. As a part of those discussions we describe certain access control and restriction services that might be appropriate for the customer.

Below, we describe certain of our products and services that aid customers in controlling access to the public network from their CPE or communications systems and in controlling access to their CPE or communications systems from the public network. None of these products/services is failsafe. None of them is guaranteed. But they are aids which customers find beneficial and helpful in managing their own telecommunications services.

a. Access Control/Restriction Services

Access restriction services are accomplished in U S WEST's central office, through translations information fed directly into the switch. They become operational based on a service order taken by U S WEST and future U S WEST actions performed on the switch. Thus, the process to render these services operational is fairly simple. And, the things that might go wrong in

a successful activation are fairly predictable, generally the result of human error.[24]

That is different than with "screening services" (discussed below). The successful operation of "screening services" involves not only a customer request, with subsequent U S WEST order activity, but certain conduct by third parties (IXCs and OSPs), and some external database or screening service. It is obvious that due to the number of variables that can affect the successful activation/operation of a screening service, such services have the built-in potential to be less reliable than access control services, as will be made more clear below.

(1) Toll Restriction and Control

In those instances warranting some kind of toll restriction,[25] U S WEST offers our customers a toll restriction service that prevents access to the toll network, including 900-type calls. When a customer dials 0 or 1 from such a restricted line,

---

[24]The predictable things that might prevent the successful operation of an access restriction service would be associated with LEC human error: the entry of incorrect information on a service order; correct service order information that becomes incorrect at the point the central office translation occurs; etc. Most of these predictable errors would, in the language of liability determinations, be deemed mistakes, i.e., they would not even rise to the level of negligence, let alone gross negligence.

[25]Such situations might include a simple inability to pay for monthly toll charges, a concern about escalating toll charges, the occurrence of "unauthorized" (although not necessarily exorbitant) toll calls, and fraud. U S WEST also offers a TeenLink service, which can be ordered with toll restriction as a part of the service.

the call is diverted to a U S WEST-provided intercept announcement.

(2) Pay-Per-Call Restriction

Even before the Commission required LECs to offer pay-per-call blocking,[26] U S WEST offered our customers such an access restriction. When such a restriction is in place, attempts to place pay-per-call transactions are diverted to a U S WEST-provided intercept announcement.

(3) International Blocking

While, theoretically, any U S WEST customer can purchase international blocking, it is most commonly purchased by large business and government users. This blocking prevents access to all direct-dialed international calls (011+ or 10XXX011+), directing the call to a U S WEST-provided intercept announcement.

(4) 10XXX1+/10XXX011+ Blocking

This service allows customers to prevent access to all alternate carrier direct-dialed domestic/international calls. When a customer dials 10XXX1+ or 10XXX011+ from a restricted

---

[26]See In the Matter of Policies and Rules Concerning Interstate 900 Telecommunications Services, Report and Order, 6 FCC Rcd. 6166, 6181 ¶ 92 (1991). See also In the Matter of Policies and Rules Concerning Operator Service Access and Pay Telephone Compensation, Order on Further Reconsideration and Further Notice of Proposed Rulemaking, 8 FCC Rcd. 2863 ¶ 1 (1993).

line, the call will be diverted to a U S WEST-provided intercept announcement.

b. Screening Services

(1) CUSTOMNET

CUSTOMNET is U S WEST's Originating Line Screening ("OLS") service. This service allows a customer to restrict certain kinds of outgoing toll calling from their stations to specified kinds of calls (e.g., only collect, third-number billed or calling card calls). When a call is placed from the premises of a CUSTOMNET subscriber, certain digits (i.e., ANI 7 digits) are provided to IXCs/OSPs as part of the originating calling line information.

While this service is clearly a valuable one for a customer trying to control calling (and, perhaps, to prevent fraud), it has certain limitations -- some technical, others of a network integration type. For example, on the technical side, CUSTOMNET is not available in U S WEST central offices serving customers with party lines, generally in Step-by-Step ("SXS") offices, in certain central offices in conjunction with Centrex/Centron-type services, and in other central offices in conjunction with certain call waiting/call forwarding features.

While technology, then, does circumscribe the availability of our CUSTOMNET offering somewhat, more fundamentally, the interplay of various network providers handling a subscriber's call can affect the successful application of CUSTOMNET. Even in